UNITED STATES DISTRICT COURT
DISTRICT OF MAINE

UNITED STATES OF AMERICA	)	
	)	
v.	)	
	)	**Crim. No. 2:14-cr-69-JDL-1**
ROMELLY DASTINOT,	)	
	)	
Defendant.	)	

ORDER ON DEFENDANT ROMELLY DASTINOT'S MOTION TO SUPPRESS

Romelly Dastinot moves to suppress wiretap evidence as violating the requirements of the Federal Wiretap Act, 18 U.S.C.A. §§ 2510-2522. ECF No. 451. Dastinot also requests a hearing pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978). *Id.* For the reasons discussed below, Dastinot's motion is denied.

I. FACTUAL BACKGROUND

On February 24, 2014, the Government submitted an application to this Court seeking authorization to intercept wire and electronic communications occurring over the cellular telephone numbers (207) 330-5654 ("Target Telephone #1" or "TT1") and (207) 713-0380 ("Target Telephone #2" or "TT2"). ECF No. 567 at 1. Accompanying the application was an 88-page supporting affidavit submitted by Task Force Agent ("Agent") Joey Brown (the "February 24 Affidavit"). *Id.* The Court granted the application, and issued an order and an amended order authorizing interceptions of wire and electronic communications occurring over both TT1 and TT2, respectively. Interception of TT1 began on February 26, 2014. *Id.* at 1-2. Interception of TT2 began on February 25. *Id.* at 2.

On March 25, 2014, the Government submitted an application to this Court seeking authorization to continue intercepting wire and electronic communications occurring over TT1 and TT2 for an additional 30 days. *Id.* The application was accompanied by Agent Brown's 83-page supporting affidavit (the "March 25 Affidavit"). *Id.* The Court granted the application and issued orders authorizing interceptions of wire and electronic communications occurring over both numbers. Interceptions pursuant to these orders began on March 25, 2014. *Id.*

On April 24, 2014, the Government again submitted an application to this Court seeking renewed authorization to continue intercepting wire and electronic communications occurring over TT1, plus authorization to intercept wire and electronic communications occurring over the cellular telephone assigned telephone number (857) 236-2924 ("Target Telephone #4" or "TT4"). *Id.* Agent Brown again submitted a supporting affidavit (the "April 24 Affidavit"). *Id.* The Court granted the application and issued orders authorizing interceptions of wire and electronic communications occurring over TT1 and TT4. Interceptions pursuant to these orders began on April 24, 2014. *Id.* at 3.

The Government submitted its final application on May 1, 2014, seeking authorization to intercept wire and electronic communications occurring over the cellular telephone number (207) 240-3478 ("Target Telephone #5" or "TT5"). *Id.* The application was accompanied by a 69-page supporting affidavit from Agent Brown (the "May 1 Affidavit"). *Id.* The Court granted the application and issued an order

authorizing interceptions of wire and electronic communications occurring over TT5. Interceptions pursuant to this authorization began on May 1, 2014. *Id.*

On December 9, 2014, a federal grand jury returned a Second Superseding Indictment against Dastinot and nine co-defendants. ECF No. 531. Count One of the Second Superseding Indictment ("Count One") charges that Dastinot conspired with at least five named co-defendants to distribute and possess with intent to distribute various controlled substances, including heroin, cocaine, and oxycodone, all in violation of 21 U.S.C.A. §§ 841(a)(1) and 846. ECF No. 531 at 1-2. Count One further alleges that the conspiracy took place in the District of Maine over a period of approximately 24 months, i.e., "not later than early 2012, and continuing until May 2014." *Id.* at 1.

Count Five of the Second Superseding Indictment ("Count Five") charges that Dastinot and one other co-defendant possessed with intent to distribute oxycodone in violation of 21 U.S.C.A. § 841(a)(1). *Id.* at 4.

Count Eight of the Second Superseding Indictment ("Count Eight") charges that Dastinot conspired with two co-defendants to launder money by engaging in transactions that "were designed in whole or in part to conceal and disguise the nature, location, source, ownership, and control of the proceeds" of unlawful activity, in violation of 18 U.S.C.A. §§ 1956(a)(1)(B)(i) and 1956(h). *Id.* at 5-7.

On October 31, 2014, Dastinot filed the instant Motion to Suppress Wiretap Evidence Under Title III and Request for a *Franks* Hearing (ECF No. 451), which was joined by co-defendants Ashley Gleason (ECF No. 454), Pierre Azor (ECF No. 466),

Carrie Buntrock (ECF No. 471), Jean Valbrun (ECF No. 475), Jonathan Duffaud (ECF No. 477), Jacques Victor (ECF No. 479), and Alcindy Jean-Baptiste (ECF No. 498).

II. MOTION TO SUPPRESS

Dastinot raises five points in support of suppressing the wiretap evidence: (A) the Government's wiretap applications failed to establish necessity; (B) the wiretap applications dated after February 2014 were based upon an illegal initial wiretap and are therefore tainted; (C) there was no necessity for additional wiretaps after the initial TT1 wiretap; (D) there was no judicial finding of necessity for any of the wiretaps; and (E) the TT1 and TT2 wiretap applications list the incorrect authorizing official, and all the wiretap applications fail to specify a particular authorizing official. ECF No. 451 at 11-19.

A. Necessity

The necessity requirement restricts wiretapping to situations where traditional investigative techniques are not sufficient to expose criminal activity. *See United States v. Rivera-Rosario*, 300 F.3d 1, 19 (1st Cir. 2002). "[A] wiretap application [must] include 'a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous.'" *United States v. López*, 300 F.3d 46, 52 (1st Cir. 2002) (quoting *United States v. Hoffman*, 832 F.2d 1299, 1306 (1st Cir. 1987)).

The necessity requirement does not require the Government to "show that other investigatory methods have been completely unsuccessful" or to "exhaust every conceivable alternative before resorting to electronic surveillance." *Rivera-Rosario*, 300 F.3d at 19. Instead, the Government need only show that "it has made 'a reasonable good faith effort to run the gamut of normal investigative procedures'" before resorting to a wiretap. *Id.* (quoting *Hoffman*, 832 F.2d at 1306). The court may also take into account the nature of the alleged crimes and give weight to the opinion of the investigating agents that other means are too dangerous and possibly counterproductive. *In re Dunn*, 507 F.2d 195, 197 (1st Cir. 1974).

Dastinot argues that the investigation "did not need wiretaps to flourish" and that investigators could have adequately uncovered the same evidence by utilizing a combination of cell site data, and both global positioning system ("GPS") and real time surveillance. ECF No. 451 at 11-16. Dastinot claims that cell site data would have pinpointed alleged sources of supply with precision because the proliferation of telecommunications base stations such as cellular towers and antennas over the past decade has caused such data to become much more accurate. *Id.* at 13-15. Dastinot also claims that Verizon Wireless, the service provider for TT1, includes a GPS chip on all phones sold after December 31, 2003, and that these GPS chips provide location information that is accurate to within 10 meters, thus obviating the need for a wiretap. *Id.* at 15-16.

Dastinot's arguments are refuted by the wiretap applications themselves. Agent Brown's February 24 Affidavit provides detailed explanations regarding why

the traditional investigative methods performed to that point had not been successful in identifying sources of supply and other significant co-conspirators. February 24 Affidavit at ¶¶ 33-50, 146-63. The Affidavit also included a detailed explanation of the shortcomings of cell site data: "Precise location information . . . cannot show who a target meets with inside of a house, the nature of any communications related to drug trafficking, or the identity of other members of the conspiracy." *Id.* at ¶ 176. Agent Brown described, at great length, the use of confidential sources and cooperating defendants to purchase drugs from Dastinot and others, that failed to "provide specific details concerning the inner-workings of this drug trafficking conspiracy and [ ] state sources of supply." *Id.* at ¶ 152. *See also, id.* at ¶¶ 150-163, 182. Agent Brown also described the Government's efforts at physical surveillance, its use of pen registers, and its financial investigation, all of which occurred prior to the wiretap application. *Id.* at ¶¶ 168-180. The Affidavit also addressed various other investigative methods that the Government had considered and rejected as being either too dangerous or too likely to alert the people being investigated of the Government's efforts. *Id.* at ¶¶ 164-167, 181-187.

Where the stated primary goal of the investigation was to identify, prosecute, and convict Dastinot's at-that-point unknown sources of supply for illegal drugs and his significant co-conspirators, *see id.* at ¶ 146, this overview of investigative efforts adequately demonstrates that the sources of supply were unlikely to be learned through traditional law enforcement techniques. The wiretap application demonstrated that the wiretaps were reasonably necessary to develop a provable case

against all significant members of the conspiracy. *See United States v. Noonan*, 2014 U.S. Dist. LEXIS 119294, at *11 (D. Me. Aug. 27, 2014).

B. Effect of Alleged Flaws in the Original Wiretap Authorization

Dastinot argues that "[s]ince the original [February 24] intercept was unnecessary here, the subsequent orders were tainted and any conversations intercepted should be suppressed." ECF No. 451 at 17. Because I conclude that the original wiretap authorization was necessary and proper, it follows that subsequent wiretap authorizations based upon the original order should not be suppressed under the theory that they are somehow tainted.

C. Diminished Necessity of Successor Wiretap Authorizations

I am also unpersuaded by Dastinot's alternative argument that even if the original February 24 wiretap authorization was legally obtained, the Government failed to establish necessity for the subsequent wiretap authorizations. *Id.* at 17 ("Rather than evaluate that information [from the original wiretap authorization] and employ traditional investigative techniques, they sought further wiretaps as a shortcut.").

Agent Brown's affidavits dating from March 25, April 24, and May 1, 2014, describe the same or similar investigative techniques as those described above from Brown's February 24 affidavit. Brown stated that law enforcement officers had used confidential sources and cooperating defendants, pen registers, physical surveillance, and financial investigation—and considered and rejected numerous other techniques ranging from undercover agents to pole cameras. March 25 Affidavit at ¶¶ 121-143;

April 24 Affidavit at ¶¶ 103-157; May 1 Affidavit at ¶¶ 81-130. As was the case with regard to the February 24 Affidavit, these affidavits also demonstrate that wiretaps were necessary to develop a provable case against all significant members of the conspiracy. *See Noonan,* 2014 U.S. Dist. LEXIS 119294, at *11.

D. Judicial Finding of Necessity

Dastinot contends that all four wiretap authorizations are deficient because they contain "boilerplate language" taken directly from 18 U.S.C.A. § 2518(1)(c), rather than an in-depth analysis and "judicial fact-finding" that, he asserts, is required by § 2518(3)(c). ECF No. 451 at 18 (citing *United States v. Giordano*, 416 U.S. 505, 533 (1974)). This argument is without merit. Section 2518 requires a judicial determination made "on the basis of the facts submitted by the applicant." 18 U.S.C.A. § 2518(3). Even if the language in each wiretap order tracks § 2518(1)(c) verbatim, that fact does not establish or suggest that the Court neglected to make a determination based upon the facts submitted by Agent Brown in his detailed affidavits, or that the Court failed to consider the results obtained by previous wiretaps, as required by *Giordano,* 416 U.S. at 533.

E. Objections Concerning the Authorizing Department of Justice Official

1. Defect in the Wiretap Application

Dastinot argues that the February 24 wiretap must be suppressed because the wiretap application names Deputy Assistant Attorney General Paul O'Brien as the Department of Justice ("DOJ") official authorizing the application, while the authorization letter attached to the application was signed by Deputy Assistant

Attorney General Kenneth A. Blanco. ECF No. 451 at 18 (citing *United States v. Reyna*, 218 F.3d 1108 (9th Cir. 2000)). Dastinot claims that this inconsistency violates 18 U.S.C.A. § 2518(1), which requires that a wiretap application list the name of the authorizing DOJ official. *Id.*

Dastinot's argument is foreclosed by *United States v. Chavez*, 416 U.S. 562, 574 (1974). Despite the error in listing different authorizing officials in the wiretap application and the authorization letter, both officials are Deputy Assistant Attorneys General. Accordingly, both may properly give authorization, and therefore "[i]n no realistic sense . . . can it be said that the order failed to identify an authorizing official who possessed statutory power to approve the making of the application." *Id.*

2. Defect in the Wiretap Order

Dastinot also notes that none of the wiretap orders state the name of the DOJ official who authorized the wiretap application, violating § 2518(4)(d). ECF No. 451 at 19 (citing *Reyna*, 218 F.3d at 1108). Dastinot argues that all four wiretap orders must be suppressed as a result. *Id.* [1]

A failure to include the identity of the authorizing DOJ official in a wiretap order constitutes a facial defect under § 2518(10)(a)(ii). *United States v. Savoy*, 883 F. Supp. 2d 101, 114 (D.D.C. 2012). However, this failure constitutes a "technical defect" that did not prejudice Dastinot or undermine the purposes of the statute. *Id.*

[1] Although Dastinot is correct that a wiretap order must state the identity of the authorizing Deputy Assistant Attorney General, *Reyna* does not support his argument because the crux of that case was the failure of federal prosecutors to secure the approval of the appropriate DOJ official *prior* to submitting a wiretap application. *Reyna*, 218 F.3d at 1111-12. The Ninth Circuit did not affirm the District Court's suppression of wiretap evidence based solely on the omission of the name of the authorizing DOJ official from the wiretap order. *See id.*

As the government notes, several courts have concluded that a wiretap order's failure to identify the person authorizing the application does not prejudice the defendant, and does not require the wiretap evidence to be suppressed. *Id.* (citing *United States v. Small,* 423 F.3d 1164, 1178 (10th Cir. 2005); *United States v. Radcliff*, 331 F.3d 1153, 1160 (10th Cir. 2003)) (other citations omitted). Thus, suppression is not necessary "where the wiretap application was authorized by an appropriate individual within the Department of Justice and that authorizing individual was identified by name in the wiretap application." *Id.* I see no sound reason to order the suppression of wiretap evidence based on the facial defect shown here.

III. REQUEST FOR A *FRANKS* HEARING

Dastinot seeks a hearing pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978), which is required when "the defendant makes a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit" and the allegedly false statement is necessary to the finding of probable cause. *United States v. D'Andrea,* 648 F.3d 1, 12–13 (1st Cir. 2011) (citation and internal quotation marks omitted). "An allegation is made with reckless disregard for the truth if the affiant in fact entertained serious doubts as to the truth of the allegations or where circumstances evinced obvious reasons to doubt the veracity of the allegations in the application." *United States v. Gifford,* 727 F.3d 92, 98 (1st Cir. 2013) (citation and internal quotation marks omitted). "In the case of allegedly material omissions, recklessness

may be inferred where the omitted information was critical to the probable cause determination." *Id.* at 98–99 (citation and internal quotation marks omitted).

Dastinot contends that Agent Brown's statements in the February 24 Affidavit regarding the unavailability of GPS data and the inability of cell site data to provide precise location information were either deliberately false or demonstrated a reckless disregard for the truth. ECF No. 451 at 20. As evidence that Brown is lying or reckless, Dastinot cites a 39-page document that purports to originate from Verizon Wireless. *Id.* at 20-21. This document describes the operations of a "Law Enforcement Resource Team" ("LERT"), a "centralized command center for all law enforcement needs," which, the document states, provides 24 hour assistance to law enforcement on matters such as electronic surveillance, call details, cell site records, and requests for location information. *Id.* at 21 (citing *http://cryptome.org/isp-spy/verizon-spy.pdf*) (the "LERT Document").

Setting aside questions about its origin and reliability,[2] the LERT document does not contradict Agent Brown's affidavit. It states that Verizon Wireless can provide the "cell site that handled [a cell phone] call," LERT Document at 10, and that it can provide "cell site, sector, and approximate distance for recently completed calls and text messages." *Id.* at 21. Nothing in the LERT Document supports the notion that cell-site data is nearly as precise as Dastinot claims, nor does it contradict

[2] Dastinot acknowledges that he "is not sure what edition LERT manuel [sic] he has is, but it appears to be from 2007 or 2008, so it is a bit dated. This manual was originally intended for law enforcement use, but several organizations have uncovered it over time, including the American Civil Liberties Union." ECF No. 451 at 21 n.4. The website Dastinot cites is not the ACLU website, and Dastinot does not identify the organization from which he obtained the LERT document.

Brown's statement that "the range of error in this type of data prevents narrowing down a precise residence (especially in dense places like Boston and Lewiston)." *See id.*; February 24 Affidavit at ¶ 175. Also, the LERT Document does not support Dastinot's assertion that Verizon Wireless could make GPS data for a particular phone available to law enforcement. *See* LERT Document at 10, 21.

Dastinot has failed to make a substantial preliminary showing that Agent Brown made a deliberately false statement, or a statement with reckless disregard for the truth, in any of the four warrant affidavits. *See D'Andrea,* 648 F.3d at 12-13. Accordingly, Dastinot's request for a *Franks* hearing is denied.

IV. CONCLUSION

For the foregoing reasons, Dastinot's Motion to Suppress and Request for a *Franks* Hearing (ECF No. 451) is **DENIED**.

SO ORDERED.

This 23rd day of March, 2015.

/s/ Jon D. Levy
U.S. DISTRICT JUDGE